Appendix O— Privacy & Security Framework: Accountability Domain

1 Introduction

The purpose of this document is to provide guidance and requirements from the perspective of Nevada's Director of the Department of Health and Human Services (DHHS Director), who is also the designated State Health IT Authority (NRS 439.587), in dealing with any breach of or other unauthorized access to the protected health information (PHI), individually identifiable health information (IIHI), and electronic health record (EHR) data being shared across the NHIE network. The document will also establish a baseline understanding of and requirements for the Accountability Standards set forth in the HIPAA Security Rule relative to dealing effectively with data breaches should they occur. It is the State's intent to model its data sharing functionality after these standards, and require all NHIE Covered Entities and participants to do the same.

In addition to directing state NHIE participants to functionally and procedurally comply with these standards for handling an individual's PHI, the Director also has a number of State-specific statutes in place for the Nevada Health Information Exchange (NRS 439.581-595), and is authorized to promulgate necessary regulations. These policies will be further detailed and developed by the State with the full NHIE governance, technology, procedures, and policies platform by mid 2013. State regulations will be developed collaboratively with the health care community during 2013, with the goal of having them enrolled by Spring 2014.

Implementation of the guidelines and requirements set forth in this document will be a function of the HIE infrastructure that NHIE will procure or subscribe to in early 2013.

2 Accountability and the HIPAA Privacy Rule

The Accountability Domain in the Privacy and Security Framework has a number of key points that, in this case, the NHIE and its Covered Entities and other participants can build upon to promote trust within the network. These points included:

- Full compliance with HIPAA and additional provisions found in State laws or regulations (such as NRS 439.581-595).
- Developing reporting mechanisms and procedures to mitigate issues any breach or mishandling of PHI/IIHI/EHR data.
- NHIE and participating Covered Entities should work closely together to assure that any communication and procedural accountability of breach issues and mitigation activities are coordinated appropriately, effectively, and in a compliant manner.

Within the realm of accountability and procedural activities mitigating breach issues, the Privacy Rule provides for considerable flexibility to Covered Entities participating in a HIE environment (see 45 CFR Sec 164.530). These provisions allow the Covered entity to develop management, accountability, and oversight structure and procedures that fit their particular operation and that are scalable to their needs. The Covered entity will

also be able to consider the most effective way to comply with these accountability and breach guidelines given their specific conditions and needs. Again, it is expected the there will be open communication and reasonable coordination with the Covered Entities (Qualified Participants) and NHIE.

2.1 Workforce Training and Sanctions

The Covered Entities (Qualified Participants and potentially other Business Associates in the HIE environment) will have policies and procedures as necessary to implement the accountability and privacy standards and to train their workforce accordingly (See 45 CFR Sec 164.530(b)). The Covered Entity also be prepared to impose sanctions for workforce members who violate the Privacy Rule or the Covered Entity's own privacy policies and procedures (See 45 CFR § 164.530(e)). The Covered Entity will need to write new privacy policies and procedures and/or adapt their existing policies and procedures to address the changes in their business practices needed to accommodate electronic sharing of PHI/IIHI/EMR. All off the Covered Entity's staff who is involved with or comes in contact with any aspect of the PHI/IIHI/EHR data being shared across the NHIE network must be trained and kept current accordingly.

2.2 Complaint Process

The NHIE as well as the Covered Entity will implement procedures which allow individuals to file complaints regarding any relevant issue(s) of compliance with the Privacy Rule, as well as its own privacy policies and procedures (See 45 CFR Sec 164.530(d)). Through this complaint procedures and processes, the NHIE and Covered Entity can learn of and address the problems and concerns of individuals with privacy practices, including concerns or problems involving the electronic exchange of PHI/IIHI/EHR across the NHIE network. A notice of privacy practices should inform individuals of how to file a complaint and provide appropriate contact information (See 45 CFR 164.520(b)(1)(vi)-(vii)).

2.3 Mitigation

Under the Privacy Rule (45 CFR Sec 164.530(f)), the Covered Entity must mitigate, to the extent practicable, any harmful effects that are known to the covered entity and that result from a use or disclosure of PHI/IIHI/EHR in violation of its own privacy policies and procedures or the Privacy Rule by the Covered Entity or its business associates. Therefore, mitigation is required where there is misuse or wrongful disclosure of PHI/IIHI/EHR data by the Covered Entity. Mitigation steps to consider can include:

- Identifying the cause of the violation and amending privacy policies and technical procedures, as necessary, to assure it does not happen again.
- Contacting the network administrator, as well as other potentially affected entities, to try to retrieve or otherwise limit the further distribution of improperly disclosed information.
- Notifying the individual of the violation if the individual needs to take self-protective measures to ameliorate or avoid the harm, as in the case of potential identify theft.

2.4 Liability for Violations of the HIPAA Privacy Rule in a Health Information Exchange Environment

Under the Privacy Rule, liability for civil money penalties arising from violations of the Privacy Rule rest exclusively on Covered Entity, even in an electronic health information exchange environment. In this case, however, more study for how this corresponds to or potentially works in concert with any state regulations or laws, such as SB-43, may be needed. As it stands, a Covered Entity participating in the NHIE will be responsible for their own non-compliance with the Privacy Rule, as well as that of their workforce. The NHIE and other participating HIEs within the statewide system that are not otherwise Covered Entities in their own right would not typically be liable for noncompliance with the Privacy Rule. However, where a Business Associate

Agreement (BAA) exists between a Covered Entity and a HIE, that HIE will be contractually obligated to adequately safeguard the PHI/IIHI/EHR data being transacted and to report noncompliance with the agreement terms to the Covered Entity. The Covered Entity will be held accountable for taking appropriate action to cure known noncompliance by the Business Associate (in this example the HIE), and if unable to do so, to terminate the business associate relationship. Pursuant to its business associate agreement, the business associate is required to extend these contractual provisions to its agents or subcontractors, as well (See 45 CFR Sec 164.502(e), 164.504(e), 164.314(a)).

2.5 Accountability and the Business Associate Agreement

The Privacy Rule requires Business Associate Agreement (BAA) to contain assurances that the NHIE organization will adequately safeguard PHI/IIHI/EHR data to be shared across the NHIE network. Some of these assurances may include that the NHIE will:

- Not use or disclose PHI/IIHI/EHR data except as allowed by the agreement.
- Implement reasonable and appropriate safeguards for PHI/IIHI/EHR data.
- Report any uses or disclosures of PHI/IIHI/EHR data that violates the agreement with the Covered Entity.

Although the Privacy Rule requires business associates to self-report to the Covered Entity uses and disclosures of PHI/IIHI/EHR data that constitute a breach or violation of the business associate agreement, the Covered Entity may want to consider other means and methods to monitor the activities of the HIE and its compliance with its Business Associate obligations. Where, through the Business Associate self-reports or based on other substantial and credible evidence, the Covered Entity becomes aware of a pattern or practice by the HIO in material breach or violation of the agreement, the Covered Entity must attempt to cure the breach or end the violation by the HIE. If such attempts are unsuccessful, the Privacy Rule would require the Covered Entity to terminate its agreement with the HIE. In the event termination is not feasible, the Covered Entity must report the HIE's (or other contracted or partnered organization) violation(s) to the Secretary of HHS through OCR.

3 Handling Breach of PHI/IIHI/EHR Data

The Nevada DHHS is taking an encompassing approach to gathering as much available information as possible on existing health information exchanges, as well as applying its own knowledge to develop this approach to dealing with breach of PHI/IIHI/EHR data. NHIE intends to handle any breach mitigation, notifications and corrective actions in compliance with all applicable federal guidelines and laws, as well as its own state guidelines that may now or at some point in the future be put in place. And, Nevada OHIT and NHIE will be advising all NHIE Covered Entities and participants to do the same. Specifically, however, breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH), including any other current state and/or federal notification laws. The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to organizations not covered by HIPAA - specifically, vendors of personal health records.

On February 17, 2009, the American Recovery and Reinvestment Act (ARRA) was signed into law. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH

significantly impacts and is imposed in conjunction with HIPAA. While HIPAA did not originally require notification when a breach of PHI/IIHI/EHR data occurred, a Covered Entity may have on its own chosen to include notification as part of its mitigation process. HITECH does require notification of certain breaches of unsecured PHI/IIHI/EHR data to the following:

- Individuals
- Department of Health and Human Services (HHS)
- Media

It should also be stated, that at the point of publishing these guidelines for breach of PHI/IIHI/EHR data, the State's governance and operational organization has not yet fully convened, nor has the State's fully functional HIE platform been selected or deployed. In that dealing with breach of PHI data requires development and adherence to organizational policy – which in this case would apply to the NHIE and each of its participating Covered Entities – any policy and guidelines suggested in this section, will be further vetted by the State's governance and operational organization at the appropriate time. But this document will be the foundation for any finalized policies and procedures adopted to address PHI breach, pending further review of the State's Governance and Operational organization, and pending any unknown state regulations that may be adopted during Nevada's 2013 Legislative session.

3.1 Definitions

Access - The ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.

Breach - The acquisition, access, use, or disclosure of PHI/IIHI/EHR data in a manner not permitted under the Privacy Rule which compromises the security or privacy of the data. For purpose of this definition, "compromises the security or privacy of the data" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI/IIHI/EHR data that does not include the identifiers listed at 45 CFR Sec 164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI. Breach excludes:

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
- Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
- A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Covered Entity (CE) - A healthcare organization of any type, including health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.

Disclosure - The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Individually Identifiable Health Information (IIHI): That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Law Enforcement Official - Any officer or employee of an agency or authority of the United States, Nevada or any other state, a territory, a political subdivision of a State or territory, or an Indian Tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Organization – (within this document) The Covered Entity to which the policy and breach notification apply.

Protected Health Information (PHI) – patient specific data which is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

Unsecured Protected Health Information – PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section
13402(h)(2) of Pub. L.111-5 on the HHS website.

1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.
    A. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
    B. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IP VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.
2. The media on which the PHI is stored or recorded has been destroyed in the following ways:
    A. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a

means of data destruction.

B. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Workforce: Workforce means employees, volunteers, trainees, and other persons whose con-duct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

3.2 Policies

Discovery of Breach

A breach of PHI/IIHI/EHR data shall be treated as "discovered" as of the first day on which such breach is known to the Covered Entity, or, by exercising reasonable diligence would have been known to the organization (includes breaches by the Covered Entity's Business Associates). The organization shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (BA) of the organization. Following the discovery of a potential breach, the organization shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been accessed, acquired, used, or disclosed as a result of the breach. The organization shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

Breach Investigation

The organization shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). Pursuant to existing Nevada state laws for the retention of medical records, all documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of 5 years, unless stipulated otherwise by state and federal laws.

NOTE: At this time, the NHIE organization has not begun hiring staff. As such, no individual is available to be named as the privacy/security officer. Currently, the DHHS Director's Office Privacy Officer has responsibility for this role relative to HIE services offered by the State.

Risk Assessment

For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, the organization will need to perform a risk assessment to

determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

- Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
- The type and amount of PHI involved.
- The potential for significant risk of financial, reputational, or other harm.

Timeliness of Notification

Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the organization involved or the business associate involved. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

Delay of Notification Authorized for Law Enforcement Purposes

If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:

- If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official.
- If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

Content of the Notice

The notice shall be written in plain language and must contain the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
- Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address. Following the formation of the NHIE organization and the hiring of staff, these specifics will be developed and deployed.

Methods of Notification

The method of notification will depend on the individuals/entities to be notified and could include the following:

- **Notice to Individual(s)** - Notice shall be provided promptly and in the following form:

- Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the organization knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.
- Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.
  - In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
  - In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organization's website, or a conspicuous notice in a major print or broadcast media in the organization's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.
- If the organization determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

- **Notice to Media:** Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.
- **Notice to Secretary of HHS (breach of more than 500 individuals):** Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the **unsecured** PHI of more than 500 patients is accessed, acquired, used, or disclosed.
  - For breaches involving 500 or more individuals, the organization shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
  - For breaches involving less than 500 individuals, the organization will maintain a log of the breaches and annually submit the log to the Secretary off HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

Maintenance of Breach Information/Log

As described above and in addition to the reports created for each incident, the organization shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach:

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.

- A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
- A description of the action taken with regard to notification of patients regarding the breach.
- Resolution steps taken to mitigate the breach and prevent future occurrences.

Business Associate Responsibilities

The business associate (BA) of the organization that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the organization of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide the organization with any other available information that the organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the organization will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity to document this notification).

Workforce Training

The organization shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.

Complaints

The organization must provide a process for individuals to make complaints concerning the organization's patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about the organization's breach notification processes. The NHIE already has consumer complaint processes in place and any of its participant Covered Entities can adopt this process.

Sanctions

The organization shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

Retaliation/Waiver

The organization may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

4 References & Resources

Supporting reference and resource materials include the following;

1) Health Insurance Portability and Accountability Act (HIPAA)

Specific sections: 160.103, 164.103, 164.501, 164.503, 164.504(e)(2)(i)(F), 164.514(e)(2), 164.526, 164.501, 164.520, 164.520(c)(3), 164.530(j)(2), 164.304, 164.306(a), 164.306(b), 164.306(b)(2), 164.308, 164.308(a)(1),164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D),164.308(a)(4), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(i), 164.310(a)(2)(ii),164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.412, 45 CFR Privacy Rule, 45 CFR Common Rule, 45 CFR 46

2) FTC Breach Notification Rules - 16 CFR Part 318

http://www.ftc.gov/os/2009/08/R911002hbn.pdf

3) American Recovery and Reinvestment Act of 2009 (ARRA)
4) Title XIII of ARRA - Health Information Technology for Economic and Clinical Health Act (HITECH) (including specifics in section 13400, Sec 164.402)
5) HHS issued guidance on protecting personally identifiable healthcare information; document was the work of a joint effort by HHS, its Office of the National Coordinator for Health Information Technology and Office for Civil Rights, and the CMS (Issued 4/17/09)
6) ONC Privacy and Security Tiger Team – various meeting notes and documents available online
7) National Institute of Standards and Technology, NIST Special Publication 800-63 Version 1.0.2

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

8) HIPAA Enforcement Rule, 45 CFR Part 160, Subpart D, and 42 CFR 1320d-5 as Amended by ARRA Section 13410(d)(3)
9) Nevada Senate Bill No. 43 (SB-43) – Committee on Health and Human Services, Changes Related to Electronic Health Records (BDR 40-443)

http://leg.state.nv.us/Session/76th2011/Bills/SB/SB43.pdf

10) Office for Civil Rights (OCR) - The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/accountability.pdf
11) Congressional Research Service – Data Security Breach Notification Laws – April 10, 2012

http://www.fas.org/sgp/crs/misc/R42475.pdf

12) The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information

http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&cachedtrue&objID=1173

http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS Framweork-5.pdf